Organisation de la SSI en entreprise

par **Robert LONGEON**
Chargé de Mission à la Sécurité des Systèmes d'Information
Direction Générale du CNRS

L'organisation de la SSI peut être vue suivant différents éclairages. On peut la voir, par exemple, sous celui de principes essentiels ; le plus important d'entre eux étant sans conteste de ne jamais oublier que la sécurité passe d'abord par les acteurs du système. Mais énoncer des principes n'est pas suffisant, il faut aussi dire quelles conséquences il convient d'en tirer sur le plan de l'organisation. C'est ce qui est fait dans le premier paragraphe pour les plus importants d'entre eux.

Dans le deuxième paragraphe, on aborde la SSI sous l'angle de l'articulation entre la technique et l'organisation, car les moyens techniques, ainsi que la sécurité, ne sont pas une fin en soi, mais sont au service d'objectifs et dans le cadre d'une entreprise ou d'une administration qui ont leurs atouts et faiblesses propres. Dans le troisième paragraphe, on passe en revue quelques structures et procédures qui, sans les poser en modèle pour tous, permettent de mieux comprendre comment mettre en œuvre une organisation de la sécurité. Enfin, dans le quatrième paragraphe on explique pourquoi on ne peut concevoir, appliquer ou piloter une politique de sécurité sans une approche méthodologique, pourquoi on ne peut mettre en place une organisation de sécurité sans commencer par une analyse de risque et en quoi les normes internationales

traitant de l'organisation, de l'administration et de l'audit de la sécurité font partie intégrante de cette approche. On termine ce paragraphe en décrivant le contenu d'un tableau de bord et son rôle dans le pilotage de la politique de sécurité qui sans cela ne pourrait que rester figée.

Quelques acronymes

SSI : Sécurité des Systèmes d'Information ; le mot « sécurité » tout seul est souvent utilisé à la place de cet acronyme.

RSSI : Responsable de la Sécurité des Systèmes d'Information.

CID : Confidentialité – Intégrité – Disponibilité est la trilogie de la SSI. On trouve dans la littérature anglo-saxonne le terme CIA (*Confidentiality, Integrity, Availability*)... tout un programme.

TI : Technologie de l'Information (IT : *Information Technology*).

ITSEC : *Information Technology Security Evaluation Criterium* (critères d'évaluation de la sécurité des technologies de l'information).

DCSSI : Direction Centrale de la Sécurité des Systèmes d'Information, service chargé de la protection des systèmes d'information au niveau de l'État.

CESTI : Centre d'Évaluation de la Sécurité des Technologies de l'Information.

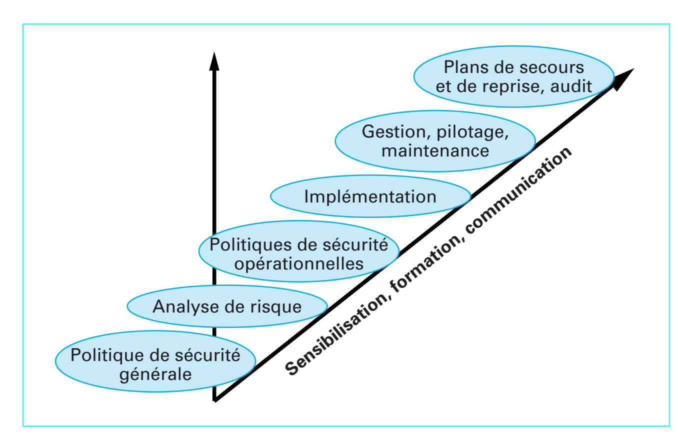


Figure 1 – Organisation de la sécurité

1. Des principes pour ne pas se tromper

Parmi les grands principes généralement cités, nous n'en retiendrons donc que quatre, ceux spécialement reliés à l'organisation de la sécurité des systèmes d'information dont on pourra trouver quelques définitions nécessaires à sa lecture dans les figures **1** et **2** et l'encadré **1**.

Encadré 1 – Qu'est-ce que la « Sécurité des Systèmes d'Information » ? (Référence ISO TR 13335-1)

C'est d'abord protéger l'information :

Confidentialité : « propriété qu'une information ne peut être accédée ou divulguée par des personnes, entités ou processus non autorisés ».

Intégrité des données : « propriété qui garantit qu'une donnée ne peut être altérée ou détruite d'une façon non autorisée ».

Intégrité des systèmes : « propriété qui garantit que la fonction attendue sera exécutée de façon complète sans manipulation non autorisée volontaire ou accidentelle ».

Disponibilité : ce service permet d'assurer l'accessibilité des informations.

C'est aussi protéger la loyauté des transactions :

Authentification : ce service permet de s'assurer de l'origine d'un message.

Non-répudiation (ou imputabilité) : ce service assure la preuve de l'authenticité d'un acte, d'une communication ou d'une transaction.

Certains sont tentés d'aller plus loin avec la « traçabilité » pour prendre en compte le développement de la mobilité, ou la « privacité » de l'information pour les aspects juridiques.

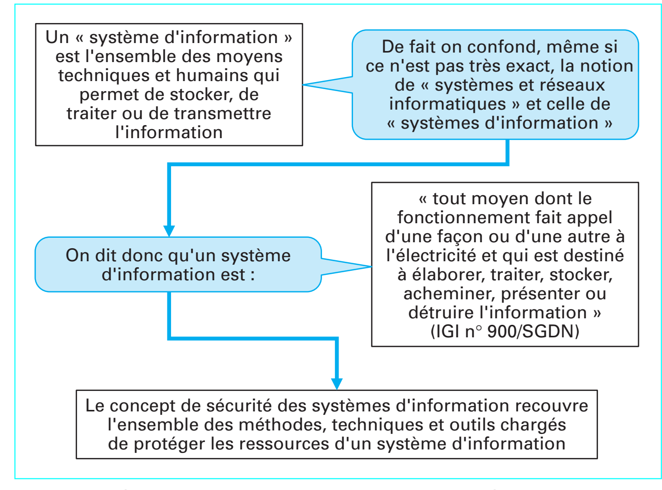


Figure 2 – Qu'est ce qu'un système d'information ?

1.1 Rôle du facteur humain dans la SSI

Le premier de ces principes est le **respect des positions relatives des hommes et des techniques dans la sécurité, les hommes au premier plan, les techniques au second**. Rien de solide ne peut se faire en SSI sans l'adhésion totale de tous les acteurs aux objectifs et aux méthodes employées, et aucun système technique, fût-il du dernier cri, ne pourra remplacer le « désir de faire », le « savoir-faire » et « l'information pour le faire ». L'organisation de la sécurité peut se résumer en un processus (figure **1**) pour lequel il faut associer à chaque étape la sensibilisation, la formation et la communication ; plus qu'un problème d'organisation, la sécurité des systèmes d'information est un problème de culture et d'individus.

1.1.1 Sensibilisation et formation

Les individus sont de plus en plus réticents aux règles, aux procédures et aux contraintes alors que les attaques contre les systèmes d'information sont plus nombreuses, leurs conséquences économiques sont plus lourdes, et les techniques les plus performantes pour leur porter atteinte sont d'accès plus facile que jamais ; la protection des circuits de décision, rendue vitale par l'exacerbation de la compétitivité économique, est sans objet si les responsables eux-mêmes n'en ressentent pas profondément l'utilité. Sensibilisation et formation doivent marcher de pair, la sensibilisation justifiant la formation et la formation permettant de délivrer des messages qui ne soient pas perçus comme pure propagande. La sensibilisation est plutôt préventive (faire prendre conscience des enjeux de la SSI) mais elle peut être aussi réactive (que faire en cas d'incident). Formation et sensibilisation peuvent s'inscrire dans une démarche ponctuelle – prendre prétexte du lancement d'un nouveau projet, de la mise en place de nouveaux matériels, de la réorganisation du service – ou permanente avec des cours planifiés de longue date. Dans ces derniers cours, une intervention, sous une forme appropriée, d'un membre de la Direction donne plus de crédibilité aux messages délivrés. La sensibilisation doit toucher toutes les catégories du personnel :

— les **dirigeants de l'entreprise** : des interventions ponctuelles et ciblées doivent pouvoir être faites en comité de Direction. On y discutera plus spécialement des aspects stratégiques de la cybercriminalité ;

— l'**encadrement intermédiaire** : les actions de sensibilisations y sont plus complexes à mener. On pourra par exemple aborder les problèmes d'organisation en se servant du tableau de bord des incidents ;

— les **utilisateurs de l'informatique** : il faut les aider à comprendre les enjeux réels de la sécurité, les axes stratégiques décidés par la Direction, les bonnes pratiques... et leur faire acquérir les réflexes de base (ne pas cliquer inconsidérément sur une pièce jointe, alerter l'administrateur système en cas d'anomalie, vérifier régulièrement les contenus de ses répertoires...). Toutefois, pour être entendu par eux, il faut savoir soi-même les écouter. Leurs interrogations, leurs remarques ou simplement leurs désirs offrent souvent l'opportunité de mettre en lumière des dysfonctionnements potentiels du système ;

— les **ingénieurs et informaticiens** : ils forment une catégorie de personnel dans laquelle on rencontre en général les plus grandes difficultés (plus de négligences et d'abus des droits, comme travailler sous le compte administrateur). On devra donc insister plus spécialement sur les outils, les procédures, la prise en compte de la sécurité dès le départ dans les projets informatiques.

1.1.2 Communication et ses supports

Avis de sécurité, charte utilisateur, planning des formations, mise en place de nouveau matériel, de nouvelles procédures (protection virale, accueil visiteurs, sauvegardes, etc.), présentation de nouvelles techniques, tout est prétexte à communiquer pour informer... et informer pour sensibiliser et former ! Les supports de la communication sont d'abord l'**Intranet** et la **messagerie électronique**. D'autres supports, comme les **CD-Rom**, les **films vidéo**, les **affiches**, sont bien adaptés à des messages plus thématiques ; une **lettre d'information interne** et un « **guide des bonnes pratiques** » constituent aussi des vecteurs très efficaces pour la communication. Ici encore, les messages doivent être adaptés à la catégorie de personnel à laquelle ils s'adressent. Par exemple, la communication vers les décideurs de l'entreprise peut exploiter les indicateurs de management : le temps nécessaire pour retrouver une activité normale après une interruption provoquée sur une machine de production, le délai moyen qui s'écoule avant de s'apercevoir d'un incident de sécurité, ou simplement le risque de perte de confidentialité de données dans des négociations en cours pour un marché. Le **tableau de bord** (§ 4.4) stratégique (indicateurs conçus pour mesurer l'application de la politique stratégique) doit avoir été conçu avec soin, aussi et d'abord dans ce but : communiquer. Un état de ce tableau de bord doit être fourni régulièrement (au moins mensuellement) accompagné de commentaires permettant d'interpréter les indicateurs et d'une synthèse.

1.1.3 Management adapté

Le rôle joué par chacun devant son poste de travail, pour la sécurité des systèmes d'information comme pour la maîtrise de la qualité, est primordial. Aussi un style de management aboutissant à l'infantilisation et, en fin de compte, à la passivité des personnels, rendra-t-il difficile la réalisation des objectifs de sécurité. Cela ne veut pas dire que la Direction ne doit pas diriger, bien au contraire – **les objectifs de sécurité doivent être clairement perçus comme émanant de la Direction** – mais que l'autorité n'est pas l'autoritarisme. Ainsi, la sécurité des systèmes d'information, reposant sur les mêmes principes de valorisation des ressources humaines que la maîtrise de la qualité (au sens ISO 9000 [21]), il est naturel qu'il en soit tiré les mêmes conclusions : il n'y a pas de sécurité possible sans un personnel correctement formé, motivé et qui se sent responsable. En particulier, la gestion des carrières peut être, si l'on n'y prend garde, une grande source de frustration, génératrice de nombreuses déconvenues, dont les moindres ne sont pas les problèmes de qualité et de sécurité [9].

1.2 Définir la SSI dont on a besoin

Le deuxième grand principe est d'**étudier et comprendre quels sont ses besoins en sécurité**. Le mot « sécurité » est ambigu en français parce qu'il fait référence au sentiment : « on est en sécurité quand on se sent en sécurité ». Alors fermons les yeux et pensons très fort que tout le monde est gentil et tout se passera bien... Ce n'est pas si sûr ! La sécurité dont on a besoin n'est pas non plus la sécurité absolue, celle qui demanderait un budget infini et l'éternité pour la mettre en œuvre ; ce n'est pas la sécurité alibi, œuvre d'ingénieurs technophiles qui croient encore qu'avec la ligne Maginot, « ils ne passeront pas » ; ce n'est pas la sécurité « tape-à-l'œil » avec le « *firewall* » en tête de réseau dont personne ne s'occupe ; enfin, ce n'est pas la sécurité vue par le technico- commercial qui vend des solutions clés en main, parce que les besoins de sécurité du voisin ne sont pas les mêmes que les nôtres. La sécurité, c'est le plus juste compromis entre le désir de contrer des menaces identifiées, constituant des risques que l'on essayera de ramener à un risque financier, et les moyens que l'on est prêt à consacrer pour se protéger. Elle se caractérise par des services répertoriés dans la norme ISO TR 13335-1 (encadré **1**) [1] [18].

1.2.1 Quelle sécurité pour mon système d'information ?

Pour définir la sécurité – bornons-nous ici à la trilogie CID de la figure **3** – dont nous avons besoin, il faut commencer par se poser les questions qui permettront d'en tracer le contour [6] [11].

Que faut-il protéger ? **Contre qui** ? **Pourquoi** ? Ces questions ont pour objectif d'identifier les menaces qui pèsent sur le système d'information.

Faut-il, dans mon système d'information, tout protéger de la même manière (fichier du personnel, base de données médicale du personnel, chaîne de traitement des salaires, etc.) ? Avant l'étude, la réponse oscille entre les deux positions extrêmes, « je ne protège rien » et « je protège tout au maximum ». La prise de conscience des menaces, les coûts de la protection ramènent en général, la réponse vers une position plus nuancée : que faut-il absolument protéger et que peut-on « moins protéger » ?

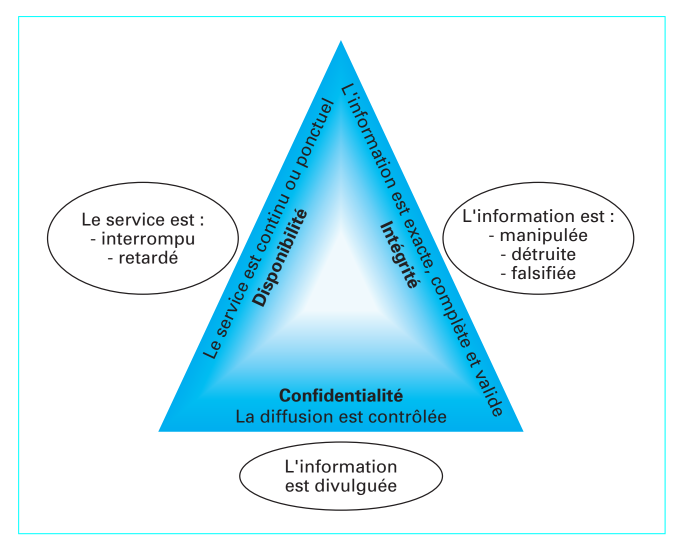


Figure 3 – La trilogie de la SSI

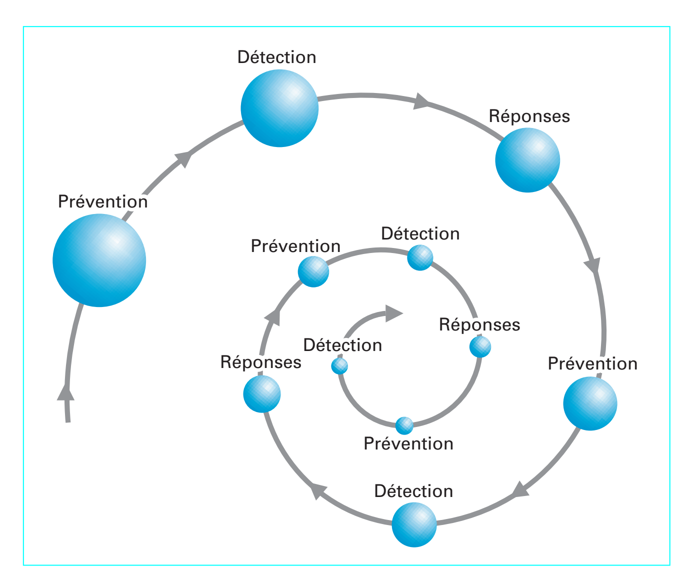


Figure 4 – Spirale de la sécurité : avec la détection, la protection de statique devient dynamique

Quel niveau de protection aurons-nous pour l'effort que nous sommes prêts à consentir et pendant combien de temps devrons-nous maintenir ce niveau ? En effet, les besoins de sécurité évoluent dans le temps : la confidentialité d'un contrat, par exemple, doit être forte tant que durent les négociations, elle peut l'être beaucoup moins après. Niveau et durée de protection sont l'expression concrète de la sécurité.

Quelle assurance avons-nous que nous sommes protégés ? C'est là un point important que celui d'avoir une « certaine assurance » que tout ce que nous avons mis en place, tous les choix que nous avons faits pour la sécurité de notre système d'information, ne sont pas que pures illusions.

1.2.2 Quels sont les moyens de la sécurité

La nature des moyens à mobiliser pour la sécurité est de trois types.

1. **Moyens humains**

Des études récentes ont montré le couplage entre les ressources humaines et les moyens techniques utilisés [22] : une augmentation des mécanismes de sécurité à ressources humaines constantes (en compétence ou en quantité) peut aboutir au résultat contraire à celui recherché ! Pour augmenter le niveau de sécurité, il faut investir simultanément dans les mécanismes de sécurité et dans les ressources humaines gérant ces mécanismes. Les délais d'adaptation plus ou moins longs de l'organisme (formation, accommodement aux nouvelles procédures, intégration de nouveaux personnels, etc.) auront pour conséquence qu'une nouvelle politique de sécurité ne pourra s'appliquer que progressivement après la mise en place de nouveaux matériels ou la remise en cause de l'organisation existante, et que la sécurité des systèmes d'information n'atteindra pas immédiatement son niveau nominal.

2. **Moyens matériels**

La réalisation de la politique de sécurité peut être accompagnée d'investissements importants qui doivent être étalés dans le temps. Cette planification sera étudiée dans le cadre d'un schéma directeur.

3. **Moyens en organisation**

La sécurité, au-delà des moyens humains et techniques, c'est surtout des procédures et de l'organisation, que l'on oublie trop souvent dans le chiffrage des coûts. En effet, la prise en compte de la SSI dans un organisme fait rarement l'économie de mesures d'organisation qui se répercutent, d'une manière ou d'une autre, sur les coûts de production. Toute réorganisation, même légère, doit être préparée soigneusement. Il faut prévoir les phases de transitions, les réactions négatives et les résistances aux changements. C'est toujours la phase la plus délicate : mal conduite elle aboutit inexorablement à de grandes difficultés dans l'application de la politique de sécurité [9]...

1.2.3 La sécurité doit s'adapter

La SSI doit être conçue comme un processus adaptatif (figure **4**) ; elle doit évoluer avec l'environnement, les besoins de sécurité, le progrès des techniques d'attaques, la découverte de nouvelles vulnérabilités. Même la perception que nous avons de la sécurité évolue : il y a quelques années, la « trilogie CID » (figure **3**) constituait la quintessence de la SSI. Aujourd'hui, avec le **développement de la mobilité** et la **prise en compte des aspects juridiques**, certains sont tentés d'aller plus loin que les cinq services définis par l'ISO 13335-1 et rappelés dans l'encadré **1** en ajoutant des services comme la « **traçabilité** » ou la « **privacité** » de l'information. Seul un système ouvert peut évoluer, seul il a la capacité de mesurer sa propre résistance aux agressions, de reconnaître les modifications de son environnement et ainsi d'offrir les moyens de son pilotage. L'approche méthodologique permet d'établir une métrique et des tableaux de bord (§ 4.4) sans lesquels il serait impossible de piloter la politique de sécurité et de sortir d'une SSI figée dans une vision établie une fois pour toutes. C'est un des arguments les plus forts en faveur d'une approche méthodologique !

1.3 La SSI est une fonction de Direction

De nombreux arguments peuvent être avancés pour justifier cette thèse, retenons-en trois [1].

1.3.1 La SSI fait partie intégrante de la stratégie de l'entreprise

La SSI engage à désigner l'ami, l'ennemi et les menaces, à décider de ce qui est important et doit être protégé, à faire des

choix d'investissements lourds. Elle nécessite une autorité pour trancher dans des conflits d'intérêt et rendre des arbitrages qui pèseront, d'une manière ou d'une autre, sur l'avenir de l'entreprise.

1.3.2 Il faut une volonté venant du sommet de l'entreprise

La SSI est une autodiscipline qui doit être entretenue, à tous les niveaux de la hiérarchie, par une détermination ferme de la direction de l'entreprise. Elle doit s'impliquer dans la définition du niveau stratégique de la politique de sécurité ; en particulier, elle doit valider l'expression des besoins, les solutions choisies, les risques résiduels et les rapports sécurité que lui propose l'équipe technique. Si elle laisse cette dernière prendre ces décisions à sa place, elle lui abandonne de fait la direction de l'entreprise.

1.3.3 La SSI exige une vision globale de l'entreprise

La sécurité est un problème global qui engage l'entreprise dans son ensemble ; c'est l'affaire de tous et tous doivent suivre la même politique, avoir les mêmes exigences, partir du même modèle de sécurité. Il ne peut y avoir de « stratégie individuelle » ou « différenciée » en la matière, seule la Direction peut tracer pour tous la route à suivre.

1.4 La SSI doit être homogène

La **politique de sécurité doit être cohérente** : rien ne sert de blinder les portes, si les fenêtres restent ouvertes ! Cet objectif ne peut être atteint :

— **sans rationalité et objectivité des choix** : il faut examiner les vulnérabilités tant sur le plan technique qu'organisationnel et humain, et avoir une approche méthodologique (§ 4) afin de ne pas se laisser entraîner par sa subjectivité ;

— **sans délimitation du périmètre de sécurité** : il faut dire clairement ce qui doit être sécurisé (l'intérieur) de ce qui n'est pas à sécuriser (l'extérieur). Cette condition est plus délicate qu'il n'y paraît : on n'est plus au temps de l'informatique centralisée où le périmètre était dessiné simplement par les murs du bâtiment qui hébergeait les machines, mais à celui des réseaux interconnectés, clients, fournisseurs, sous-traitants, filiales, aujourd'hui amis, demain concurrents. Comment situer les frontières dans ces conditions ? Où commence l'extérieur [14] ?

2. Techniques

Nous ne nous arrêterons pas sur les aspects purement techniques qui font l'objet d'autres articles du traité sur la Sécurité des systèmes d'information, mais relevons simplement les concepts suivants.

2.1 Les premières causes des incidents de sécurité ne sont pas d'ordre technique

Quand on recherche les origines des incidents de sécurité dans une entreprise [16], on s'aperçoit qu'ils sont majoritairement encore d'origine interne et que pour les attaques d'origines externes, les principales vulnérabilités utilisées sont :

— la présence de logiciels d'écoute des mots de passe sur des réseaux hôtes lors de connexions distantes ;

— une mauvaise gestion des comptes utilisateurs, comme les mots de passe triviaux ou les comptes restés ouverts après le départ de l'entreprise du titulaire du compte ;

— une mauvaise configuration du système ou des accès réseaux non contrôlés ;

— l'utilisation de failles de sécurité connues sur les systèmes parce que les correctifs n'ont pas été appliqués.

D'où le constat que les premières causes des incidents de sécurité sont d'ordre **« organisationnel » et humain**. Aussi est-ce d'abord sur ces facteurs qu'il faut agir. D'ailleurs, l'expérience montre que les réponses purement techniques aux problèmes de sécurité ne permettent d'apporter que des réponses automatiques à des attaques connues et répertoriées. Elles permettent au mieux de contenir une délinquance qui utilise des outils tout faits, trouvés sur Internet, mais nullement de lutter contre une criminalité informatique autrement plus sérieuse, comme celle provenant de concurrents sans scrupule.

2.2 Associer organisation et technique pour trouver des solutions spécifiques

Les besoins de sécurité, la capacité à y répondre, les réponses que l'on y apporte, dépendent étroitement de la culture de l'entreprise, de l'état de l'existant, d'aspects économiques et sociologiques divers de l'organisme. En sécurité, les problèmes sont concrets et les solutions sont toujours spécifiques, alors que les mécanismes techniques offrent une réponse générique à un problème théorique. Ils ne satisferont donc jamais – seuls – les besoins de sécurité.

2.3 Absolue nécessité de structurer le réseau

À cheval entre la technique et l'organisation, la première des mesures à prendre est la structuration du réseau (figure **5**).

2.4 Défenses en profondeur

De la grande muraille de Chine faite pour contenir les invasions mongoles, à la ligne Maginot, l'histoire le démontre : les murs sont faits pour être franchis, les blindages pour être percés. Aussi le problème essentiel en sécurité n'est pas celui d'être attaqué – même avec succès –, mais celui de la nature et de la rapidité de la réaction. Les mécanismes techniques ont certes leur utilité en « défense passive », comme blindage du réseau, mais ils l'ont davantage encore dans la mise en œuvre de « **sécurités actives** ». Tout accès à un service réseau doit être contrôlé, authentifié, filtré, tracé ; l'efficacité de la politique de sécurité doit être évaluée par des indicateurs (failles résiduelles sur les systèmes, pourcentage de mots de passe faibles, tentatives d'intrusion...) et le système doit pouvoir répondre par des actions correctives programmées à un incident de sécurité : arrêt de session, reconfiguration dynamique des systèmes de contrôle d'accès, enregistrement des sessions, etc. ; il faut surveiller les moyens de protection et contrôler leur efficacité ; détecter les attaques et les mauvaises configurations (enregistrement des accès aux services sensibles, mise en place de systèmes de détection d'intrusions, de leurres, etc.). En cela, les mécanismes techniques de sécurité complètent harmonieusement les mesures d'organisation.

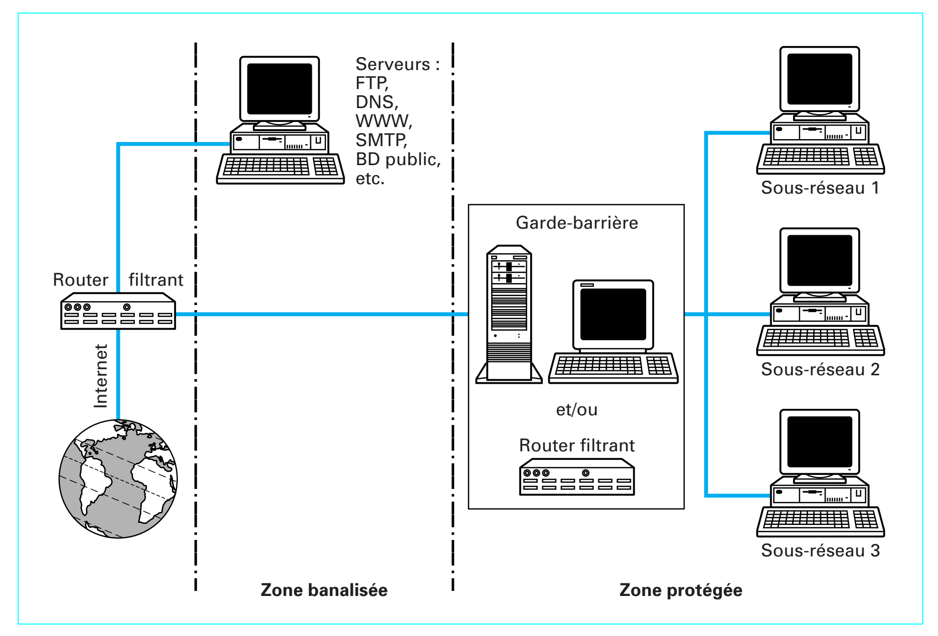


Figure 5 – Structurez vos réseaux

3. Structures et procédures

Parmi les éléments d'organisation, commençons par citer les **structures**, c'est-à-dire les organigrammes hiérarchiques et fonctionnels, et les **procédures**, ensemble des règles, des formalités, qui doivent être observées, des actes qui doivent être accomplis lors de certaines opérations effectuées au sein de l'entreprise et ayant un caractère normatif. Les méthodes d'introduction de la SSI dans une organisation, plus particulièrement les techniques de conduite du changement, ont beaucoup à emprunter à l'expérience acquise dans le domaine de la qualité [9].

3.1 Exemple d'une structure SSI

3.1.1 Niveaux de responsabilité

Dans un groupe multiétablissement, une organisation de la sécurité peut se décliner sur trois niveaux, le niveau central, le niveau établissement (local) et éventuellement un niveau « correspondant » (service). Lorsque l'entreprise est monoétablissement ou lorsque les liens entre les différents établissements sont assez lâches, le niveau central et le niveau établissement se confondent simplement.

Le **niveau central**, directement rattaché à la direction générale, doit assurer la cohérence des politiques locales, la coordination des actions (formation et sensibilisation centralisée, élaboration de documents généraux, planification des moyens), l'élaboration et la mise en œuvre de la politique stratégique (figure **6**), la remontée des informations et la réalisation du tableau de bord stratégique pour le comité de direction. Il ne faut surtout pas, à ce niveau, mobiliser des effectifs pléthoriques ; quelques individualités (suivant l'importance de l'entreprise) motivées et correctement formées, responsables, matérialisant clairement l'engagement de la Direction dans la SSI, se révèlent en général extrêmement efficaces.

Le **niveau local** est le pendant du niveau central – mêmes fonctions – pour la gestion du système d'information de chaque établissement (il est donc situé à un niveau plus opérationnel). Il est en plus l'interlocuteur direct du niveau central et son relais dans l'établissement, le gestionnaire des droits localement, et il anime le réseau de correspondants. C'est le RSSI (responsable de la sécurité des systèmes d'information) de l'établissement.

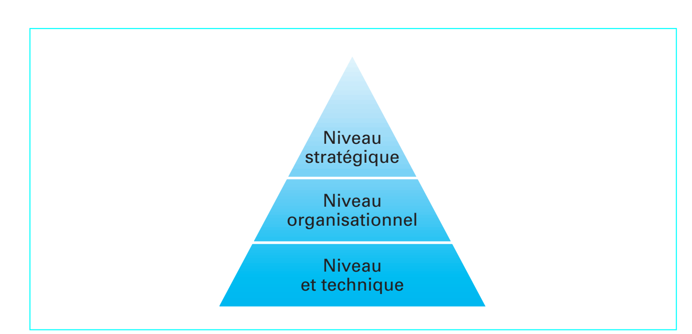


Figure 6 – Les niveaux de la politique de sécurité

Le **réseau de correspondants** est la cheville ouvrière de la sécurité dans l'entreprise, c'est le niveau le plus opérationnel sur le terrain. Il veille à la bonne application, à la vérification et à l'adaptation de la politique de sécurité. Il est en relation directe avec le RSSI de l'établissement. Il est administrateur système, gestionnaire de base de données ou responsable des applications (pour nous limiter à l'aspect purement informatique de la SSI).

3.1.2 Réseau de RSSI

Dans un groupe multiétablissement, une telle organisation aboutit à la mise en place d'un réseau de RSSI dont la **responsabilité de l'animation** revient à la structure centrale : organisation de séminaires thématiques, journées SSI périodiques permettant de faire le point avec tous les RSSI sur les problèmes en cours, mise en place de groupes de travail traitant de thèmes spécifiques, rédaction d'une revue et de documentations, etc. C'est par la qua-

lité de cette animation que les RSSI d'établissement ressentent l'intérêt de la Direction générale pour leur travail, qu'ils se sentent soutenus et reconnus et qu'ils maintiennent la mobilisation dans leur établissement. Toute défaillance de cette animation se répercute immanquablement à la base par un relâchement de la sécurité.

3.1.3 Dépendance hiérarchique d'un RSSI

Le RSSI, au niveau central comme au niveau de chaque établissement, est **rattaché directement à la Direction générale**. Comme pour le contrôle de gestion ou pour une mission d'audit, au-delà de l'aspect symbolique de la mesure – signifier l'importance accordée à la sécurité –, c'est un grand principe du droit : « on ne peut être juge et partie ». Un rattachement à la Direction informatique, tentation à laquelle beaucoup d'entreprises succombent, fait perdre aux RSSI toute liberté de jugement des projets de celle-ci et les transforme le plus souvent en simple « faire-valoir ».

3.2 Exemples de procédures et règles

3.2.1 Mise en place d'une application

La mise en exploitation d'une modification ou d'une nouvelle application doit donner lieu à :

— une vérification de la conformité aux spécifications et de la sécurité de l'application, en s'appuyant sur les méthodes de développement utilisées (procédure de recette d'une application) ;

— une analyse des droits sur les données utilisées et produites ;

— une analyse des droits liés à l'installation et à l'exploitation de l'application ;

— la mise en place de l'organisation permettant la gestion de ces droits à la validation des décisions leur inférant. Pour certains organismes dans lesquels l'accès aux applications ou aux données qu'elles utilisent est « sensible » (le secteur bancaire par exemple), on pourra nommer un gestionnaire de droit qui en réfère au RSSI.

3.2.2 Gestion des comptes utilisateur

Il faut mettre en place les procédures de gestion de compte des utilisateurs : ouverture d'un compte, fermeture d'un compte, vérification des mécanismes d'authentification (solidité des mots de passe par exemple), vérification des comptes « dormants », etc.

3.2.3 Gestion du parc informatique

La gestion du parc comprend, outre la **cartographie complète du réseau**, la tenue d'un **inventaire, matériels et logiciels**, la **vérification des espaces disque installés** et le **contrôle d'accès aux périphériques**, une procédure pour l'installation ou la connexion d'une nouvelle machine sur le réseau. Chaque machine doit être administrée d'une manière explicite par un responsable en titre. L'activation des lecteurs de disquettes et de CD est soumise à autorisation et il faut une procédure pour l'administration et la gestion des licences de logiciels et des contrats de maintenance. Les prises réseau inutilisées doivent être neutralisées.

3.2.4 Accès aux systèmes d'informations

3.2.4.1 Accès physique

L'accès physique aux machines, particulièrement aux serveurs, aux équipements d'extrémités du réseau et à l'autocommutateur doit être strictement contrôlé : toute machine pouvant être manipulée par des **personnes non autorisées** ne peut être sécurisée et par là, c'est le réseau auquel elle est connectée qui se trouve en danger (encadré **2**).

Encadré 2 – Sécurité physique

Les moyens techniques sont au service d'un objectif et dans le cadre d'une organisation. C'est pourquoi, avant de penser « quelle technique ? », il faut penser « quelle organisation pour quel objectif ? ». La sécurité physique, même si elle tend à devenir moins obsessionnelle que dans la période où l'informatique était centralisée, demeure tout aussi cruciale : un système, un serveur ou un réseau (fût-il sans fil) dont on ne peut assurer le contrôle d'accès est très difficile, sinon impossible à sécuriser. Les premières mesures de sécurité sont donc des mesures d'organisation pour empêcher les personnes non autorisées à approcher les équipements :

➔ l'accès physique à tous les composants du système (serveurs, câbles, équipement d'interconnexion de réseaux...) doit être contrôlé ;

➔ des zones « particulières » ou « sensibles » à accès très limité peuvent éventuellement coexister avec des zones moins restrictives au sein d'un même système d'information ;

➔ il faut déconnecter les machines sensibles du réseau et désactiver les lecteurs de disquettes et de CD-Rom quand ils ne sont pas indispensables ;

➔ il est indispensable que le PABX soit confiné dans une pièce sécurisée ;

... et pensez à avoir un plan de secours contre le feu, les inondations, la tempête, etc.

Nota : PABX, Private Automatic Branch eXchange (central téléphonique privé).

3.2.4.2 Accès réseau

L'accès réseau aux systèmes informatiques peut être soumis à une procédure supplémentaire pour assurer la **confidentialité des données de connexion**, plus particulièrement pour celles distantes. Rentrent dans cette catégorie la télémaintenance et les accès aux systèmes par des consultants externes (externalisation de la sécurité, infogérance, par exemple). Dans chacun de ces cas, il est raisonnable d'avoir soigneusement analysé les risques induits d'une consultance comparativement aux avantages qui en découlent et négocié correctement le contrat de fourniture de la prestation : des clauses sur l'accréditation des opérateurs, l'enregistrement, l'exploitation et la conservation des traces des activités, la définition précise du périmètre d'intervention s'imposent.

3.2.5 Traitements des incidents

Le traitement des incidents fait l'objet de plusieurs procédures, pour mémoire citons :

— les procédures d'alerte (qui doit être informé et par quel moyen ?) ;

— les procédures d'urgence en cas de malveillance (déconnecter la machine du réseau, enregistrer une image du système, des journaux, des traces...) ;

— les procédures de repli permettant de continuer l'activité en mode dégradé pendant les vérifications et la restauration du système ;

— les procédures de remise en service permettant de retrouver progressivement une activité normale ;

— les procédures de bilan et de remontée d'incident.

3.2.6 Sauvegardes

Il est important de préciser clairement les règles qui doivent être respectées dans les sauvegardes : leur type et leur périodicité, comment doivent-elles être faites en fonction des machines, quels sont les critères de vérification à observer et comment les conserver.

3.2.7 Règles de diffusion de l'information

L'information est une richesse dont il faut pouvoir contrôler la diffusion : quelles sont les informations qui peuvent être diffusées, par quels moyens doivent-elles l'être, qui peut le faire et qui peut être destinataire (le « besoin d'en connaître »).

4. Méthodes

Plusieurs approches de la SSI sont possibles. La première, la plus simple, est l'approche purement technique, sans politique de sécurité explicite : on ne veut absolument pas toucher à l'organisation existante, juste installer un dispositif qui permette, par exemple, de **filtrer les flux**, de **journaliser les demandes de service** ou de **partitionner le réseau**. C'est une sécurisation reposant sur des systèmes automatiques et correspondant à un « modèle » de sécurité prédéfini que l'on applique « intuitivement » sans études préalables. Pauvre, sans spécification, demandant peu d'effort de conception et de mise en œuvre, il n'offre de couvertures que contre une menace de faible intensité. Protège-t-il contre une malveillance interne ? A-t-on envisagé toutes les conséquences d'un incident de sécurité ? Sait-on comment faire la reprise d'activité après un sinistre ? Ces questions, et bien d'autres, laissées sans réponses resurgiront avec force le moment venu. Cette manière de voir résulte des concepts, encore très prégnants, hérités d'une autre époque, celle de l'informatique centralisée et autonome où la sécurité pouvait se limiter aux contrôles des accès physiques aux machines. Il faut tourner la page et comprendre qu'aujourd'hui, il n'y a pas d'ouverture possible du réseau sans une « politique de sécurité explicite », que celle-ci ne peut se concevoir sans une approche méthodologique comportant une analyse de risques [8] [10] et qu'enfin, la politique de sécurité doit être pilotée afin de l'adapter à l'environnement qui se modifie en permanence. L'instrument de ce pilotage est le **tableau de bord de sécurité** [11] [15] [18].

4.1 Exigences essentielles de toute approche méthodologique

La nécessité d'une approche méthodologique pour élaborer la politique de sécurité s'est faite sentir très tôt. C'est dès le début de la décennie 1980 qu'en France, le CLUSIF proposa la méthode MARION (Méthodologie d'Analyse des Risques Informatiques et d'Optimisation par Niveau) qui, bien que ne traitant que du risque statistique utilisé surtout dans l'assurance, avait le mérite de donner une certaine cohérence à la politique de sécurité. Depuis, de nombreuses autres méthodes ont été proposées ; on ne pourra pas dans le cadre de cet article toutes les citer. Il est du reste difficile de tracer une frontière claire entre des méthodes servant à « implémenter », gérer ou auditer la sécurité, car on ne crée que rarement une organisation de sécurité « *ex nihilo* » ; on part généralement d'un « existant » dont on fait l'étude en recherchant ce qui doit être amélioré, élagué ou réalisé pour atteindre les objectifs de sécurité que l'on s'est fixés.

Les méthodes d'audit de la SSI sont nombreuses – parfois une méthode est spécifique à tel cabinet de consultant – mais heureusement elles ont en commun des exigences que nous rappelons brièvement :

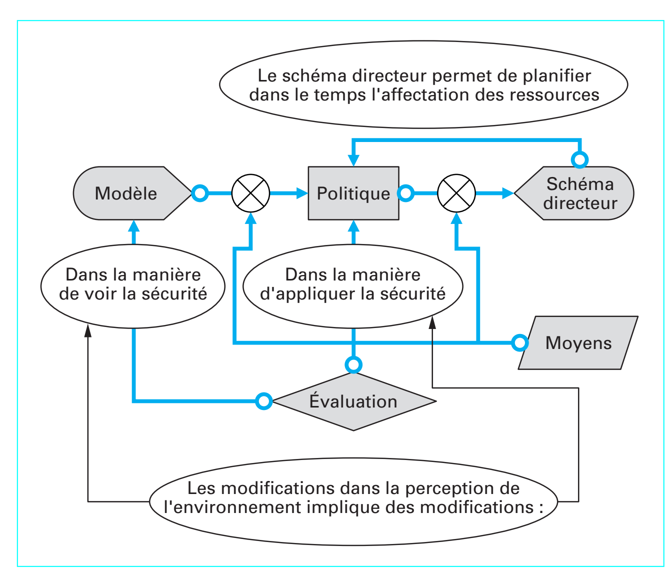


Figure 7 – Fonctionnement du schéma directeur

— définir le périmètre de ce qui est à sécuriser suivant la criticité du système ;
— définir la granularité du système ;
— formaliser l'existant en mettant l'accent sur les objectifs stratégiques, les processus fonctionnels, les flux et interfaces et les infrastructures techniques ;
— mener des entretiens avec les acteurs du système d'information pour valider la situation existante et mieux comprendre les attentes ;
— réaliser un schéma directeur (figure **7**) : planification des investissements et de mise en place des structures.

D'une manière plus générale, dans toute méthode digne de ce nom, il est nécessaire de différencier les phases du cycle de vie du système d'information et de procéder à une analyse de risque.

4.1.1 Différencier les phases du cycle de vie d'un SI

On peut distinguer différentes phases dans la création d'un système d'information en fonction de la nature des travaux qui sont à réaliser. Elles peuvent être plus ou moins détaillées dans le cadre de la méthode adoptée. Ce sont ces différentes phases qui constituent le cycle de vie du système [7] [15]. Par exemple, le cycle de vie simplifié de type ITSEC [2] [23] en distingue quatre : la spécification des besoins, la conception, la réalisation et l'utilisation.

■ **Spécification des besoins**

La spécification des besoins est retranscrite dans un document que l'on appelle « **cahier des charges fonctionnel** ».

On commence par décrire les objectifs poursuivis et les obligations qui doivent être satisfaites : solutions imposées ou interdites, coûts, délais, normes, réglementations, culture d'entreprise, etc., mais on ne doit pas y présumer des solutions techniques qui seront retenues. La description des objectifs met en évidence les besoins de sécurité du système d'information en termes de stratégie, d'impacts du niveau de la SSI sur les performances de l'entreprise, de pertes maximales pouvant être supportées, de contraintes dues à l'environnement physique et organisationnel, de menaces

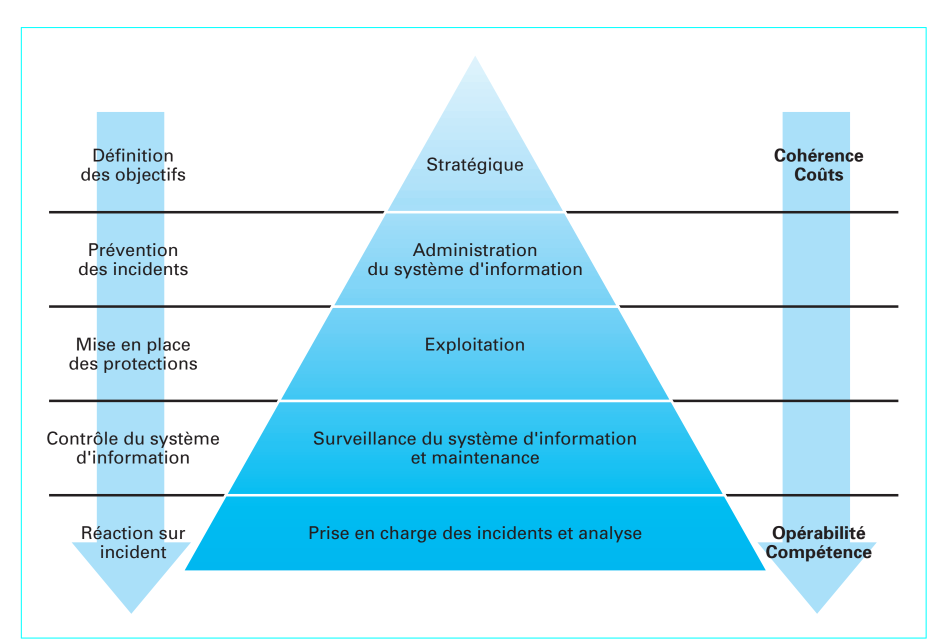


Figure 8 – Administration de la sécurité

vitales. Au cours de cette phase sont identifiés les domaines opérationnels concernés et définies les grandes caractéristiques du système d'information :

— **objectifs stratégiques** et fonctionnels, services qu'il doit rendre ;

— **contexte** dans lequel celui-ci va être utilisé ;

— **relations avec l'extérieur** ;

— **limites** du système à concevoir.

Enfin, durant cette phase, on examine les menaces spécifiques et les vulnérabilités associées aux éléments connus ou supposés (les services « en ligne » ne peuvent pas être empêchés de fonctionner pendant plus d'un quart d'heure, les personnes ayant accès à la base de données doivent être authentifiées d'une manière sûre, les données comptables ne doivent pas être modifiées par une personne non autorisée), pour en déduire les objectifs de sécurité, juste compromis entre ces éléments et les moyens, par nature limités, que l'entreprise est prête à dégager pour se protéger. Les objectifs de sécurité se concrétisent par des mesures organisationnelles et des mesures techniques de sécurité exprimant ce qui reste à couvrir par des fonctions techniques.

■ **Conception**

Durant cette phase, au cours de laquelle est défini ce que sera le système, le concepteur (ou le maître d'œuvre) élabore une solution globale adaptée aux exigences formulées dans le cahier des charges fonctionnel. Il la formalise sous la forme des **Spécifications Techniques de Besoin**. Ce document comprend quatre parties :

— étude de l'existant mettant en évidence les points forts et les points faibles, tant du point de vue technique qu'organisationnel, du système à sécuriser ;

— analyse des besoins exprimés par le maître d'ouvrage dans le cahier des charges fonctionnel par rapport à cet existant ;

— étude des solutions ;

— bilan de faisabilité et le choix d'une solution.

C'est à ce stade qu'il faut définir la politique d'administration de la sécurité (figure **8**), les procédures de sauvegarde et d'alertes, le mode de fonctionnement dégradé et les plans de retour à l'activité normale.

■ **Réalisation**

C'est la phase qui comprend l'ensemble du processus d'installation du système et de configuration des mécanismes de sécurité sur le site d'exploitation. Elle commence par l'acceptation par le maître d'ouvrage de la solution retenue et se poursuit jusqu'à la recette, en passant par les phases de tests des éléments constitutifs qui ont été acquis ou développés, la validation globale, la formation des futurs responsables de la sécurité du système et le retrait du service existant.

■ **Utilisation**

C'est la dernière phase du cycle de vie : elle comprend l'exploitation, la maintenance du système (administration de la sécurité du système, gestion des sauvegardes, test périodique du plan de secours) et les contrôles pour s'assurer de la pérennité et de l'efficacité des mesures de sécurité. Des missions d'audit de sécurité doivent être menées régulièrement par des acteurs extérieurs afin de contrôler dans le temps le respect de la conformité et de l'efficacité de la sécurisation du système par rapport aux besoins et aux objectifs de sécurité exprimés.

La sécurité, quand elle est pensée dès le début du cycle de vie d'un système d'information, est à la fois plus facile à mettre en œuvre et plus efficace pour un coût considérablement moindre.

4.1.2 Procéder à une analyse du risque

Les exigences de sécurité d'un système d'information découlent de l'analyse du risque, probabilité qu'une menace particulière puisse exploiter une vulnérabilité donnée, provoquant un dommage estimé en unités monétaires (figure **9**) [7] [10]. L'**évaluation du coût de ce dommage** n'est pas toujours aisée : interruption d'activité d'une entreprise consécutive à une destruction accidentelle d'informations, divulgation d'une information stratégique, perte d'image ou de crédibilité d'une entreprise qui a laissé porter atteinte à son système d'information, préjudice moral à une personne ; dommage à un bien ou à une propriété intellectuelle, doute sur l'intégrité de données consécutif à un accès non autorisé à une machine, etc., c'est pourtant de sa précision et de son

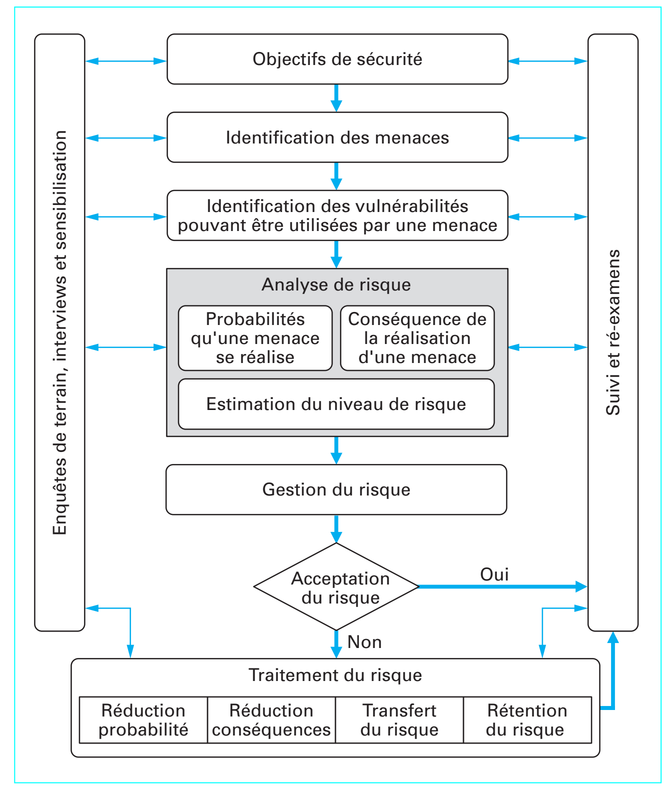


Figure 9 – Analyse et gestion du risque

exactitude que dépendra la pertinence des principaux choix de sécurité faits par la suite. Aussi faut-il ne jamais être prisonnier de ses propres raisonnements et garder un œil critique sur les conclusions que l'on est amené à tirer de l'analyse de risque.

Une telle évaluation peut être faite par « **une approche descendante** » encore appelée « approche par scénarios » qui cherche à identifier les menaces globales qui pèsent sur les systèmes d'information et analyse leur mode de réalisation, ou par « **une approche ascendante** » qui part du besoin de protection (plus particulièrement CID comme indiqué figure **3**) des « composants élémentaires du système d'information » pour remonter vers les scénarios d'attaque. Les deux approches sont complémentaires. Le terme « de composants » du système d'information suppose ici d'avoir défini au préalable une décomposition cellulaire. La décomposition cellulaire relève de deux nécessités contradictoires, celle de différencier les modes de mise en œuvre des services de sécurité dans la mesure où ils ne peuvent s'appliquer de la même manière et avec le même niveau d'adéquation dans toute l'entreprise, et celle de limiter le volume de travail à fournir pour mener à bien l'étude. Plus le niveau d'agrégation est fin, plus précis est le résultat... et complexe l'analyse !

4.1.2.1 Identifier les menaces

Les menaces peuvent être **naturelles**, **accidentelles** ou **intentionnelles** : pannes, accidents, sinistres, catastrophes, erreurs humaines (dont les plus fréquentes sont les erreurs de conception d'un système), malveillances internes et attaques externes. Elles évoluent dans le temps, comme évoluent les techniques, les architectures, l'environnement social, le périmètre de sécurité, les enjeux, la réglementation, les vulnérabilités elles-mêmes. Il s'en suit que le risque se modifie en permanence et que la politique de sécurité ne peut être rigidement définie une fois pour toutes : elle doit mesurer l'évolution du risque et s'adapter.

4.1.2.2 Identifier les vulnérabilités par la méthode de listes de contrôle

Les listes de contrôle récapitulent les vérifications à réaliser. Pour la détection des vulnérabilités informatiques, il faut utiliser un **logiciel d'audit de vulnérabilité**.

À titre d'**exemple,** citons le logiciel de Renaud Deraison, Nessus http://www.nessus.org/download.html qui est gratuit, Saint qui a une version gratuite et une version commerciale ftp.cerias.purdue.edu et ISS scaner ftp.cerias.purdue.edu qui est payant.

L'utilisation de standards et de procédures dans les activités ordinaires permet de circonscrire la variété des vérifications à effectuer.

4.1.2.3 Évaluer les risques

Ainsi l'évaluation d'un risque consiste-t-elle à déterminer la probabilité d'apparition d'une menace par l'exploitation d'une vulnérabilité et l'impact qu'elle aurait dans cette hypothèse sur le système d'information. Plusieurs méthodes permettent d'effectuer cette étude. Citons les deux principales en France : **EBIOS** (acronyme pour « Expression des Besoins et Identification des Objectifs de Sécurité ») [4] dont on peut obtenir une documentation complète sur le site de la DCSSI, et **MEHARI** (MÉthode Harmonisée d'Analyse de Risques) qui a été élaborée par le CLUSIF [2] (CLUb de la Sécurité des systèmes d'Information Français).

4.1.2.4 Autres méthodes

À ces deux méthodes, MEHARI et EBIOS, très complètes, on pourrait en ajouter d'autres [24]. Trois de ces méthodes, pour des raisons diverses, sont souvent citées dans les réunions internationales ou par les cabinets de conseil :

— **BS 7799-2** (the Specification for Information Security Management) du British Standards est la deuxième partie de la norme BS7799, celle qui n'a pas été normalisée par l'ISO. Elle se présente comme une méthode d'audit mais traite essentiellement de l'analyse de risque [26] ;
— **CORAS** propose un modèle de spécifications pour l'analyse de risque [25]. Cette méthode a été conçue dans le cadre d'un projet européen ;
— **EMR** (Évaluation de la menace et des risques) : approche canadienne de l'analyse de risque. Une présentation complète de la méthode est disponible sur Internet [27].

4.2 Normes d'administration de la sécurité

L'analyse de risque est le cœur de toute démarche méthodologique, mais elle n'épuise pas toute la question. L'ISO a normalisé différents apports sur l'organisation de la sécurité des systèmes d'information. Ces normes font partie intégrante de l'approche méthodologique. Les plus importantes sont :

— ISO 17799 qui est un code de bonnes pratiques [17] ;
— ISO 15408 (dit « Critères Communs ») [19] plus spécifique à la certification et l'assurance sécurité [5] ;
— ISO/IEC TR 13335 qui pourrait s'apparenter à un guide (indispensable) de la sécurité [18].

4.2.1 ISO 17799

L'ISO 17799 est la normalisation de la première partie du BS 7799. Cette norme est un code de « **bonnes pratiques** » de la sécurité en dix leçons [17] :

1. la politique de sécurité ;
2. l'organisation de la sécurité : infrastructure de la sécurité de l'information, sécurité des accès par des tiers, sous-traitance ;
3. la classification et la maîtrise du capital informationnel ;
4. la sécurité du personnel : sécurité dans la définition des postes et des ressources, formation des utilisateurs, réactions aux incidents de sécurité et aux mauvais fonctionnements ;
5. la sécurité physique et la sécurité de l'environnement : zones de sécurité, sécurité du matériel, mesures de maîtrise générales ;
6. la gestion des communications et des opérations : procédures et responsabilités opérationnelles, planification et recette des systèmes, protection contre les logiciels malveillants, intendance, gestion des réseaux, manipulation et sécurité des supports, échanges d'informations et de logiciels ;
7. la maîtrise des accès : exigence de l'entreprise concernant la maîtrise des accès, gestion des accès utilisateurs, maîtrise des accès aux réseaux, maîtrise de l'accès au système d'exploitation, maîtrise des accès aux applications, surveillance des accès aux systèmes et de leur utilisation informatique mobile et télétravail ;
8. le développement et la maintenance des systèmes : exigence de sécurité des systèmes, sécurité des systèmes d'exploitation, commandes cryptographiques, sécurité des fichiers systèmes, sécurité des environnements de développement et de soutien ;
9. la gestion de la continuité des activités professionnelles ;
10. la conformité : conformité aux exigences légales, revues de la politique de sécurité et de la conformité technique, considérations concernant les audits des systèmes.

4.2.2 ISO 15408

Un groupe de travail du nom de « **Critères Communs** » a été créé pour faire converger les approches européennes et américaines d'évaluation des TI (« produits et systèmes des Technologies de l'Information ») et définir une « échelle commune d'assurance de sécurité » [12]. Ces travaux ont débouché sur un rapport normalisé en juin 1999 sous le label ISO 15408. Cette norme, dite aussi « **Critères Communs** » ou CC (du nom du groupe de travail), offre un outil intéressant à tous ceux qui doivent assumer la responsabilité de la protection des informations et des systèmes (figure **10**). Elle donne les moyens – bien mieux que les ITSEC [23] avant elle – de juger de l'aptitude d'un produit ou d'un système à assurer sa fonction de sécurité, à condition toutefois de connaître quelle est la cible de sécurité du TI, d'avoir étudié le rapport de certification... et d'avoir déterminé ses propres objectifs de sécurité. La norme présente les exigences sur la sécurité des TI sous deux formes distinctes : les exigences fonctionnelles et les exigences d'assurance. Les exigences fonctionnelles décrivent le comportement de sécurité souhaité et les fonctionnalités de sécurité que peut mettre en œuvre un produit. Les exigences d'assurance, base pour acquérir la confiance, établissent que les mesures de sécurité sont conformes aux spécifications et sont efficaces. L'assurance de sécurité est le résultat d'une évaluation consignée dans un rapport. Rapport et norme garantissent le sérieux de l'évaluation en précisant entre autres les cinq points suivants.

Quelle partie du produit ou quelles propriétés spécifiques ont été vérifiées ?

Les produits sont très variés et répondent à des besoins très différents ; leurs propriétés de sécurité doivent donc être décrites avec précision suivant un processus que détaillent les Critères Communs. Un utilisateur de TI a déterminé une menace contre laquelle il désire se protéger (« l'incursion dans un lieu sensible par une personne non autorisée ») ; il décide d'une « politique de sécurité technique » (« on utilisera l'authentification biométrique ») ; ce faisant, il émet des hypothèses sur le produit (« je suppose que l'on peut avoir confiance dans les données biométriques »). Cette phase s'appelle la description de l'environnement de sécurité. Elle débouche sur une définition des objectifs de sécurité. Il faut

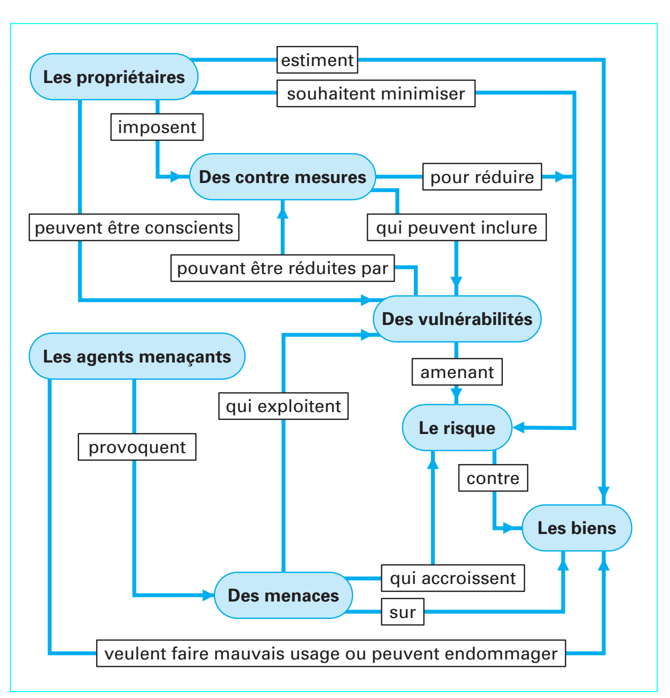


Figure 10 – Concepts de sécurité et relations dans les Critères Communs

ensuite formaliser cette réflexion en décrivant les exigences de sécurité de telle manière qu'elles soient compréhensibles aussi bien par l'industriel que par l'organisme de certification. Les Critères Communs offrent une liste de près de 150 spécifications prédéfinies, non ambiguës, ne dépendant pas de l'implémentation et personnalisables – appelés « composants » – et organisées hiérarchiquement en familles et en classes. Ils définissent aussi la structure des profils de protection (PP) qui permettent aux utilisateurs et aux développeurs de créer des ensembles normalisés d'exigences de sécurité pour satisfaire leurs besoins. La cible de sécurité dans les Critères Communs est cet ensemble : environnement, spécifications, fonctions. Définir la sécurité d'un produit, c'est définir sa cible de sécurité.

Comment est effectuée cette vérification ?

Les méthodes utilisées, leur objectivité, leur reconnaissance par une communauté assez large légitiment la confiance. L'évaluation montre soit que les revendications sont fausses, soit qu'une démarche « sécurité » a été observée tout au long du processus de réalisation du produit, de la conception à la fabrication. Les Critères Communs offrent la prédéfinition de près de 75 conditions à vérifier pour assurer la fonctionnalité revendiquée dans la « cible de sécurité ».

Quelle confiance peut-on avoir dans les vérificateurs ?

Que vaut le certificat qui a été délivré ? Pour certains, le certificat n'a de valeur que dans la mesure où il est « garanti par le gouvernement » ; pour d'autres, « seul un certificat émis par un service de l'entreprise est sûr » ; pour d'autres encore, ils ne feront confiance qu'à tel organisme qu'ils ont su apprécier par ailleurs. Mais, pour qu'au niveau international une reconnaissance mutuelle soit possible, il faut une procédure d'homologation des organismes certificateurs qui soit la même pour tous et ne prête pas le flanc à suspicion. C'est l'objet de la norme ISO 17025 [20]. En **France**, l'**homologation est attribuée par la DCSSI**. Le schéma de

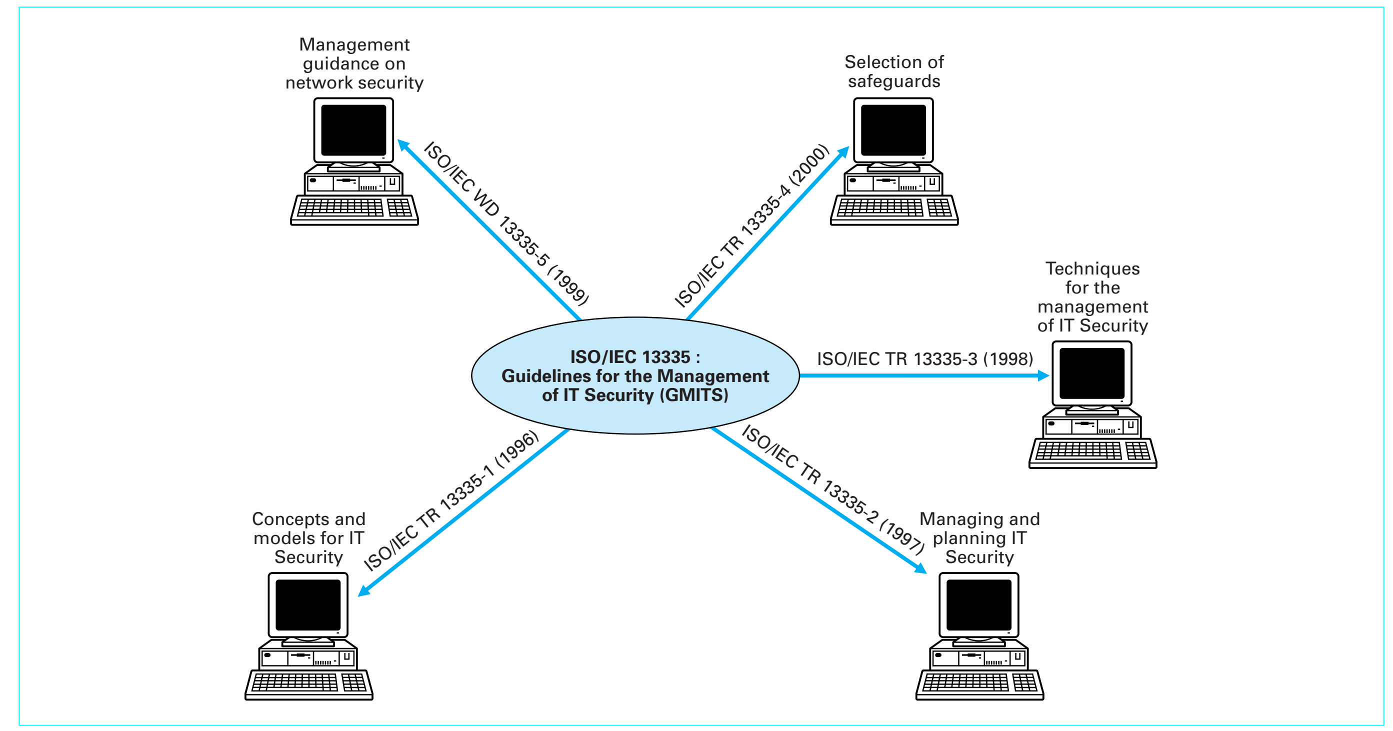


Figure 11 – Les cinq parties du GMITS

certification a été conçu pour garantir la qualification et l'indépendance du certificateur. Les contrôles *ad hoc* ont été mis en place pour garantir la valeur des certificats émis afin de bloquer toute possibilité de certificats de complaisance. Que penser de la pertinence technique des évaluateurs ? Le schéma d'évaluation envisage ce point en organisant un contrôle périodique de la qualité du travail des CESTI ; toutefois, l'évaluateur peut être confronté à certains travaux en marge de leur expertise, particulièrement pour la partie d'analyse de vulnérabilités. Les évaluations sont réalisées à la réserve près que les tests de vulnérabilités soient effectués suivant l'état de l'art du moment : il est donc toujours possible que des vulnérabilités résiduelles subsistent dans le produit évalué - certifié.

■ **Où trouver la liste des produits certifiés ?**

Les sites des différentes autorités de certification nationales offrent une information complète. La **DCSSI**, pour sa part, procure aujourd'hui la liste exhaustive des produits certifiés, mais pas celle des produits en cours de certification.

■ **Quels sont les documents publics associés aux certifications ?**

Le rapport de certification émis par l'organisme certificateur est public. Ce rapport donne des indications succinctes sur le périmètre de la cible de sécurité, sur la cible d'évaluation, sur les principales conclusions de l'évaluation et éventuellement sur les recommandations d'usage du produit évalué. Attention, on ne trouvera pas tout le détail de l'évaluation dans ce rapport afin de ne pas apporter d'indication susceptible d'aider d'éventuels attaquants. Le plus souvent, la cible de sécurité est également disponible sur le site de l'autorité certificatrice. Ce document – plus encore que le rapport de certification – permet de comprendre l'étendue des travaux effectués et la portée réelle de l'évaluation. Il existe une très grande disparité entre les cibles de sécurité, car si les CC sont stricts sur le fond, ils laissent une liberté importante sur la forme de ce document. Il faut noter que la DCSSI a engagé un effort méritoire pour que les cibles des produits certifiés soient relativement aisées d'accès. Les éditeurs cherchant à valoriser les certificats obtenus, il n'est pas rare de trouver sur leurs sites des informations précieuses sur le contexte d'usage des produits ou systèmes certifiés.

4.2.3 ISO 13335

La norme ISO/IEC 13335, dite aussi GMITS pour « *Guidelines for the Management of IT Security* », est un **guide d'administration** de la sécurité des technologies de l'information. Elle est découpée en cinq parties (figure **11**) :

1. concepts et modèles pour la sécurité des technologies de l'information ;
2. management et planning de sécurité des technologies de l'information ;
3. techniques pour la gestion de sécurité des technologies de l'information ;
4. sélection de sauvegardes ;
5. guide pour la gestion de sécurité du réseau.

C'est un document indispensable pour tout RSSI.

4.3 Politique de sécurité

De l'analyse de risque, on en vient naturellement à la gestion du risque : c'est l'objet de la politique de sécurité. « *Une politique de sécurité est un ensemble de règles et principes régissant la gestion de biens, informations et ressources sensibles. Concrètement, c'est s'organiser, c'est-à-dire connaître ses besoins et ses objectifs de sécurité, dégager des moyens humains et matériels, définir puis appliquer des procédures* » [2]. Les risques ayant été évalués, les

politiques de sécurité (figure **6**) auront pour objet d'agir sur ce risque soit :

— par la réduction de la probabilité de réalisation de la menace : « la structuration de mon réseau diminue le risque d'intrusion sur mes machines de production » ;

— par la réduction des conséquences que pourrait avoir celle-ci : « en cas de panne d'un disque dur, j'ai des sauvegardes conservées dans l'autre aile du bâtiment » ;

— par le transfert du risque : « mon assurance incendie me permettra de retrouver une partie de mon capital en cas de sinistre » ;

— par la rétention du risque : « j'accepte d'assumer la persistance de certains risques qui me coûterait trop cher à éliminer ». C'est le risque résiduel ;

— par l'évitement du risque : les menaces inacceptables pour l'entreprise, celles qui même à faibles probabilités mettraient son existence en danger, devront être soit transférées, soit éliminées.

4.3.1 Rendre explicite la politique de sécurité

La SSI consiste à vérifier que la politique de sécurité n'est pas – ou n'a pas été – violée. Si la politique de sécurité n'est pas explicite, que peut signifier « la sécurité » pour les acteurs du système ?

4.3.2 Déclinaison de la politique de sécurité

L'étude de la sécurité d'un système d'information part des objectifs de sécurité et aboutit à des mesures d'ordre organisationnel et technique. *« Si l'organisation a été correctement pensée en fonction d'objectifs réalistes, la mise en place des mesures techniques se fait naturellement. La difficulté devient rapidement insurmontable lorsque l'on essaie de greffer des mesures techniques ou des procédures sur une organisation qui n'a pas été prévue pour cela »* [2]. C'est la raison pour laquelle on a, dans la figure **6**, différencié trois niveaux de mise en œuvre d'une politique de sécurité :

4.3.2.1 Niveau stratégique

La politique de sécurité stratégique est un document général qui décrit les objectifs globaux de sécurité et donne la doctrine à suivre. Il ne doit pas faire plus de quatre pages. Les deux derniers niveaux, organisationnel et technique, ont pour raison d'être la réalisation de la politique stratégique.

4.3.2.2 Niveau organisationnel

La politique de sécurité, à ce niveau, explicite les structures de la SSI et détermine les responsabilités. Elle énonce les procédures à suivre, les standards à respecter et les règles à observer. C'est à ce niveau que sont définis :

— les plans de secours et de retour à l'activité après incident ;
— les mesures préventives ;
— la charte utilisateurs : respect des lois, respect de l'éthique, respect des règles particulières ;
— les audits de sécurité ;
— le rôle et les « privilèges » de chacun ;
— la documentation de la SSI ;

et que l'on met en place les plans de la sensibilisation et la formation.

4.3.2.3 Niveau technique

À ce niveau, la politique de sécurité fait les choix techniques sur les moyens de protection [13]. Elle étudie également :

— la mise en place des alertes ;
— la détection des vulnérabilités ;
— le contrôle actif du système ;
— la vérification de la conformité de l'état réel de la sécurité avec les exigences de sécurité ;
— la prise en charge, les analyses et les rapports d'incidents ;
— la veille technique.

Concevoir une bonne politique de sécurité n'est pas suffisant, il faut aussi une fenêtre ouverte sur la réalité du monde qui évolue et change à grande vitesse. Cette fenêtre, c'est le tableau de bord.

4.4 Tableau de bord

4.4.1 Rôle d'un tableau de bord

Le tableau de bord a plusieurs fonctions. Nous avons vu combien il est erroné de s'enfermer dans une vue statique de la sécurité, tant dans les objectifs poursuivis que dans les moyens employés. Il est l'outil d'administration de la sécurité (figure **8**) et permet l'adaptation de la politique de sécurité en donnant des informations sur son efficacité, les modifications de l'environnement, l'apparition de nouvelles faiblesses, le risque résiduel du système et son évolution, sous la forme d'indicateurs, d'alarmes, de compteurs divers. Cette **adaptation** se fait suivant des constantes de temps différentes selon le niveau de la politique de sécurité qu'elle concerne. Le niveau stratégique est le plus stable (on ne change pas d'objectifs de sécurité tous les jours !), tandis que le niveau technique est plus changeant.

C'est grâce à la production de mesures opérationnelles synthétisée par les tableaux de bord qu'il est possible de lier un niveau de sécurité à un niveau de risque. Les directions peuvent maintenant contrôler l'efficacité de la politique et percevoir concrètement les enjeux de la sécurité. La sécurité n'est plus ressentie comme un trou noir dans lequel s'engouffrent sans fin les crédits ; ce ne sont plus des dépenses obligatoires et stériles. Ainsi peuvent-ils traiter la sécurité comme n'importe quel autre investissement. Sans tableau de « bord sécurité », la Direction ne peut que laisser les techniciens décider pour elle.

Le tableau de bord est aussi un outil de communication, d'information et de sensibilisation. L'adhésion de tous les acteurs aux objectifs de sécurité est un objectif réaliste, même vis-à-vis de ceux qui n'ont pas un niveau d'expertise élevé, mais il leur faut une information claire. Le tableau de bord, en apportant une **« vision » de l'état de sécurité du système à chaque instant**, donne réellement le moyen à chacun de participer pleinement aux processus de sécurité.

4.4.2 Contenu d'un tableau de bord

Les indicateurs sont à étudier attentivement de façon à donner des informations de synthèses pertinentes sur l'état de la sécurité : on ne trouve que ce que l'on cherche. Aussi le tableau de bord est-il lié à l'administration de la sécurité telle qu'elle est représentée figure **8** et présente-t-il des aspects différents suivant le niveau considéré :

— **au niveau stratégique** : il faut des indicateurs notamment pour situer le système d'information par rapport à celui des principaux concurrents, pour donner un aperçu des incidents majeurs et leurs conséquences, pour mettre en évidence certains dysfonctionnements du système d'information, etc. ;

— **au niveau « administration du système d'information »** : il faut des indicateurs synthétisant l'évolution des risques (probabilité et impact d'une menace) tels qu'ils ont été mis en évidence lors de l'analyse de risque [3]. Il faut imaginer ces indicateurs en se servant des questionnaires de la phase d'analyse de risque qui a abouti au choix des politiques de sécurité ;

— **au niveau exploitation** : ce sont des alarmes et des données vérifiant les différentes techniques de mesure et de prévention des incidents ;

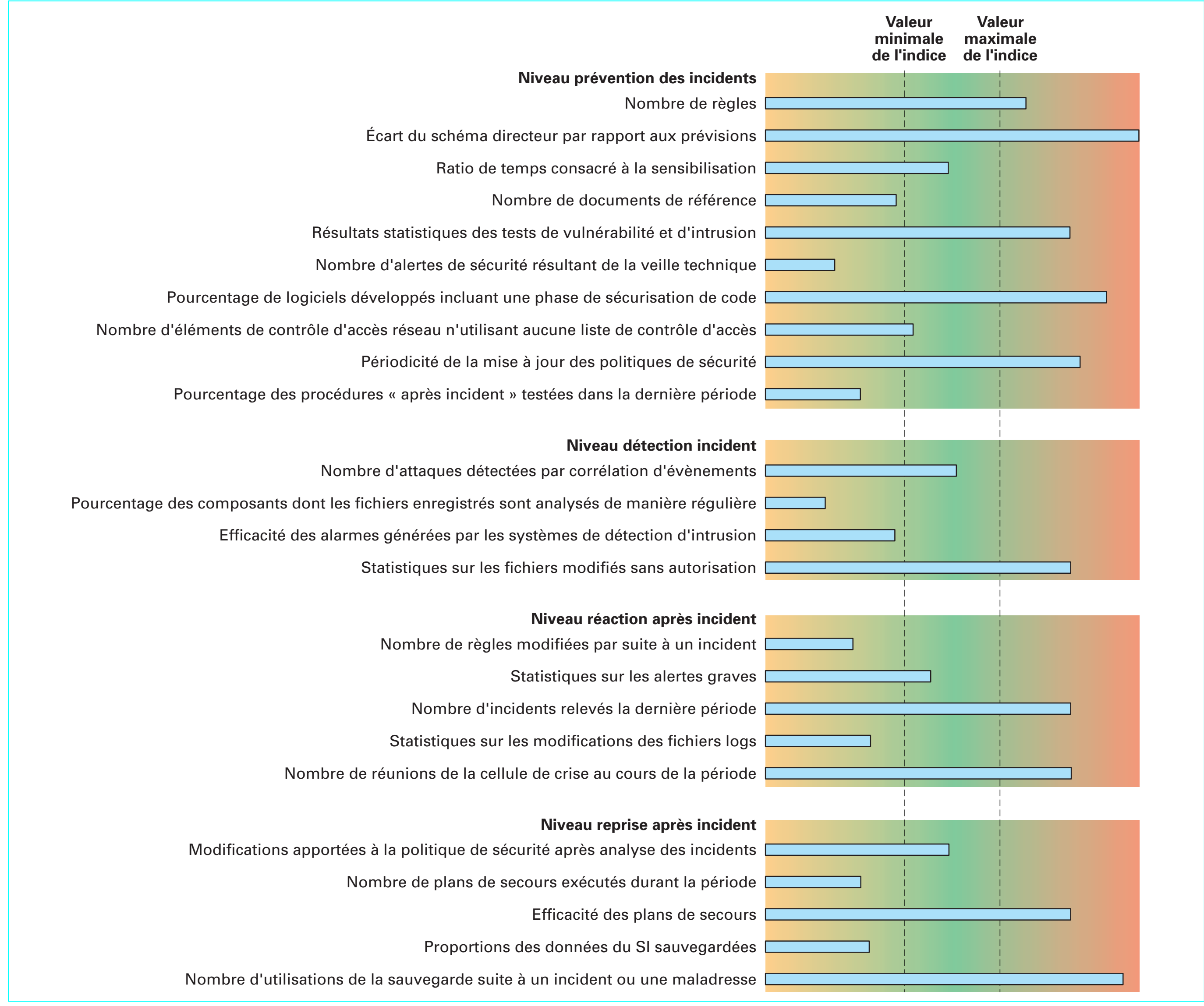


Figure 12 – Tableau de bord de la politique sécurité

— **au niveau « surveillance du système et maintenance »** : il faut des indicateurs synthétisant les données des détecteurs d'intrusion, d'audit de failles, de vérification d'intégrité des systèmes, d'analyseurs réseau, des traces de connexion et d'accès aux services, de détecteurs de scans, détecteurs de ports ouverts, d'analyse de robustesse de mots de passe, etc. [13] ;

— **au niveau « prise en charge des incidents et analyse »** : il faut des indicateurs mesurant la réactivité à un incident, la pertinence et la bonne application des plans de secours et de reprise d'activités normales, la remontée des informations sur les incidents, etc.

La conception d'un tableau de bord est une opération lourde qui de surcroît est à renouveler régulièrement. La mise en œuvre, le fonctionnement et l'interprétation des indicateurs demandent aussi beaucoup de professionnalisme. Autant de difficultés qui peuvent amener certains à vouloir s'en passer. Ils ont tort, c'est un composant essentiel de la sécurité : sans tableau de bord, ils appliquent une politique de sécurité sans rien savoir de son efficacité, ils sont aveugles !

Des **exemples** de tableau de bord sont donnés par les figures **12** et **13**.

5. Conclusion

Répondre aux exigences de sécurité ne signifie pas que vous pouvez être sûr à 100 % que les objectifs de sécurité que vous vous êtes fixés seront atteints. Cela signifie seulement que vous contrôlez votre sécurité : vous détectez les attaques en un temps « raisonnable », vous vérifiez vos procédures régulièrement et êtes capable d'en déceler les défauts, vous tirez des leçons des incidents de sécurité, vous journalisez les accès aux services réseau, etc. En une phrase : vous gérez votre sécurité.

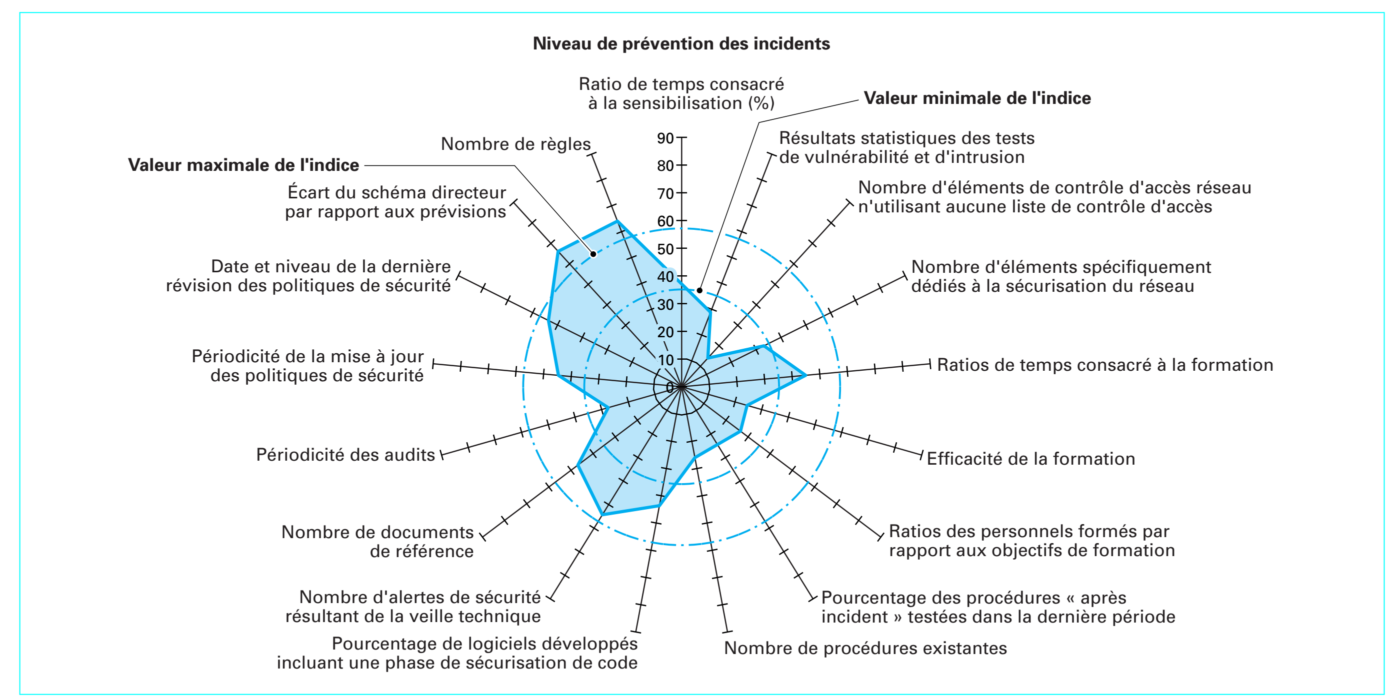


Figure 13 – Tableau de bord de la politique sécurité

Références bibliographiques

[1] *Sécurité informatique : manager et assurer.* AFNOR normes, fév. 2002. http://www.afnor.fr

[2] CLUSIF et MEHARI. – août 2000. http://www.clusif.asso.fr

[3] CLUSIF. – *Les indicateurs de sécurité,* juil. 2001. http://www.clusif.asso.fr

[4] DCSSI. – *La méthode EBIOS* (1996). http://www.ssi.gouv.fr/fr/confiance/ebios.html

[5] DCSSI. – *Critères Communs* (1999). http://www.ssi.gouv.fr/fr/confiance/cc21.html

[6] *Information Security Risk Assessment Guide.* – Practices of Leading Organizations, US General Accounting Office - Exposure Draft.

[7] JOUAS (J.-P.). – *Risque informatique : modélisation, évaluation.* Red, Édition d'organisation, oct. 1992.

[8] GEFFROY (J.-C.). – *Sûreté des fonctionnements des systèmes informatiques.* Masson, oct. 1998.

[9] GOGUE (J.-M.). – *Management de la qualité.* Economica (2001).

[10] LAPRIE (J.C.). – *Guide de la sûreté de fonctionnement.* Cepadues, mai 1995.

[11] LONGEON (R.) et ARCHIMBAUT (J.-L.). – *Guide de la sécurité des systèmes d'information à l'usage des directeurs.* CNRS (1999). http://www.cnrs.fr/Infosecu/guide/guide.pdf

[12] LONGEON (R.). – *La confiance dans la sécurité des systèmes numériques.* Sécurité informatique, mai 2002. http://www.cnrs.fr/Infosecu/num42.pdf

[13] McCLURE (S.), SCAMBRAY (J.) et KURTZ (G.). – *Hacking Exposed : Network Security Secrets & Solutions.* Third Edition, John Wiley & Sons (1994).

[14] MEINADIER (J.P.). – *Ingénierie et intégration des systèmes.* Hermes, oct. 1998.

[15] NIEL (E.) et CRAYE (E.). – *Maîtrise des risques et sûreté de fonctionnement des systèmes de production.* Hermes, fév. 2002.

[16] OCDE. – *Guidelines for the Security of Information.* Organization for Economic Cooperation and Development (1992) – dernière mise à jour (1997).

Norme ISO http://www.afnor.fr

[17] ISO/CEI 17799 : Technologies de l'information - Code de pratique pour la gestion de sécurité d'information (2000).

[18] ISO/IEC TR 13335 : Guidelines for the management of IT Security, (GMITS) – Part 1 : Concepts and models for IT Security (currently under revision) – Part 2 : Managing and planning IT Security – Part 3 : Techniques for the management of IT Security – Part 4 : Selection of safeguards – Part 5 : Management guidance on network security (1996).

[19] ISO/IEC 15408 : Information technology. Security techniques. Evaluation criteria for : 1 Introduction and general model, 2 Security functional requirements, 3 Security assurance requirements (1999).

[20] ISO/IEC 17025 : General requirements for the competence of testing and calibration labora (1999).

[21] ISO 9000 : Quality management systems. Fundamentals and vocabulary (2000).

Références indisponibles actuellement

[22] ANDERSON (A.). – *La sécurité des systèmes d'information en l'An 2000.* 1re et 2e parties, juin 2000.

[23] *Information Technology Security Evaluation Criteria.* Version 1.2, Commission of the European Communities, juin 1991.

Quelques sites importants

[24] http://csrc.nist.gov/publications/history/index.html

[25] http://www.nr.no/coras/

[26] ISO/IEC 17799 : Frequently Asked Questions (2000) : http://csrc.nist.gov/SBC/PDF/ISO_IEC_17799_2000_Inf_Sec_Mgmt_FAQ.pdf

[27] http://www.cse-cst.gc.ca/fr/documents/knowledge_centre/publications/itsg/mg3f.pdf